VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA ÚČETNICTVÍ

Elektronický podpis a jeho alternativy

Electronical Signature and its Alternatives

Student: Tereza Franková

Vedoucí bakalářské práce: Ing. Marcela Palochová, Ph.D.

Ostrava 2011

„Místopřísežně prohlašuji, že jsem celou práci vypracovala samostatně a uvedla jsem všechny použité podklady a literaturu.“

Děkuji Ing. Marcele Palochové, Ph.D a Ing. Josefu Praksovi za odborné vedení bakalářské práce.

V Ostravě dne: 9.5. 2011

……

Vlastnoruční podpis

OBSAH

1. Úvod

V dnešní době je elektronický podpis běžnou záležitostí, je možno se s ním setkat v podstatě na každém kroku. Elektronický podpis je používán pro přihlašování do internetového bankovnictví, pro komunikaci se státní správou, ale i při přihlašování do různých internetových aplikací. Firmy dnes běžně používají pro komunikaci mezi sebou elektronický podpis. Elektronický podpis nám z jistého hlediska zjednodušuje život, ale zároveň nám přináší rizika. Znalost problematiky elektronického podpisu je často podceňována, což způsobuje možné problémy hlavně z pohledu bezpečnosti. Rizika napadení elektronického podpisu jsou dnes velká, a řekla bych stále se zvyšující. Proto se elektronický podpis stále vyvíjí, aby těmto hrozbám byl schopný odolat. Dnes je možné svou identifikaci potvrdit pomocí scannerů otisků prstů, vzorků hlasu atd. Toto zní trochu jako science fiction, ale k ochránění našich soukromých dat je to nutné. Problematika elektronického podpisu je velmi zajímavou záležitostí, proto jsem si tuto oblast vybrala jako téma pro svou bakalářskou práci.

Ve své bakalářské práci se zabývám elektronickým podpisem jako samostatnou kategorií, historií vzniku, důvody a případy užití, včetně výčtu běžně užívaných metod z pohledu zákona i metod alternativních. Ve své práci rovněž analyzuji důvody použití alternativních metod pro elektronické podepisování. Praktickým cílem mé práce je srovnání metody SMS autorizace vůči třem dalším metodám běžně užívaných ve finančním sektoru. Porovnání metod je provedeno zejména z hlediska bezpečnosti, uživatelského komfortu a nákladů na implementaci a provoz.

Úvodní část bakalářské práce je zaměřena na definování základních pojmů, v oblasti chápání elektronického podpisu, jeho legislativní rámec a případy využití.

Další část je zaměřena na oblast používaných a nově navržených metod. Dále se zabývá srovnáním těchto metod z hlediska bezpečnosti, porovnáním vlastností metod z pohledu uživatele, použitelnosti metod pro různé obslužné kanály.

V praktické části bude řešený obchodní model přechodu na jiné metody autentizace, efektivnost investice, dále pak finanční model a business case.

Vlastní komentáře, návrhy, připomínky jsou v bakalářské práci psány kurzívou.

2. Problematika elektronického podpisu

2.1 Historie a vývoj využívání elektronického podpisu a alternativních metod

Pojem digitální podpis vznikl souběžně s rozšířením asymetrické kryptografie v druhé polovině sedmdesátých let - toto rozšíření bylo způsobeno mezi jiným i významným nárůstem výpočetního výkonu v IT. Elektronický podpis (dále v textu i e-podpis) tak, jak je známý dnes, je obecnějším pojmem než digitální podpis. E-podpis nabízí kromě samotného digitálního podpisu ve formě certifikátu také možnost použití biometrické metody, které se využívají pro autorizaci legislativních dokumentů a pro komunikaci s orgány státní správy. Ve světě obvyklé RFID, u nás je užívaná biometrie například v nové generaci cestovních dokladů - pasů.

2.2 Legislativa

Elektronický podpis je v rámci Evropské unie upraven směrnicí 1999/93/EC Evropského parlamentu a Rady Evropské unie o zásadách Společenství pro elektronické podpisy. Směrnice se zabývá elektronickými podpisy používanými především pro účely autentizace a aplikací zaručených elektronických podpisů, které mají být rovnocenné klasickým, ručně psaným podpisům. Směrnice také stanovuje požadavky, které mají být splněny poskytovateli služeb, kteří podporují elektronické podpisy a další požadavky vztahující se k podepisující straně.

Směrnice je do českého právního řádů transponovaná zákonem č. 227/2000 Sb., o elektronickém podpisu. Zákon o elektronickém podpisu je základním právním předpisem, který upravuje používání elektronického podpisu.

K tomuto zákonu existuje prováděcí vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb. Dále s elektronickým podpisem úzce souvisí problematika elektronických podatelen, která je upravena nařízením vlády č. 496/2004 Sb. k elektronickým podatelnám a vyhláškou č. 496/2004 Sb., o elektronických podatelnách.

Dále se elektronickým podpisem zabývá zákon č. 40/1964 Sb., občanský zákoník, dále pak zákon č. 337/1992 Sb., o správě daní a poplatků ve znění pozdějších předpisů.

2.3 Využití elektronického podpisu

Elektronický podpis lze využít všude tam, kde je zapotřebí vlastnoruční podpis. Veškeré dokumenty je možné převést z papírové podoby na dokumenty elektronické a všechny podpisy převést na jejich elektronickou formu. Výhodou je, že je možné opatřit podpisem i to, co ručně podepsat nelze – obsah diskety, fotografii v souboru, textový soubor atd.

2.4 Využití a trendy v používání dalších zabezpečovacích zařízení a metod

2.4.1 Hesla

Autentizace pomocí hesla je v dnešní době jedním z nejjednodušších způsobů autentizace. Přesto, to neznamená, že tento způsob autentizace je naprosto bezpečný. I když tento způsob představuje určitá rizika, je používán velkým množstvím aplikací. Příkladem jsou protokoly pro připojování k poštovním serverům, ICQ pro komunikaci přes internet atd.

Typické pro heslo je řetězec dlouhý 6-10 znaků. Uživatel předkládá systému heslo zároveň se svou identifikací – uživatelským jménem. Systém tyto autentizační údaje kontroluje s daty, které jsou uloženy k danému uživateli. Prokázání znalosti sdíleného tajemství je nutno, aby systém vyhodnotil korektní prokázání identity. [4]

2.4.2 Osobní identifikační čísla – PINy

PINy poskytují další z možností posílení bezpečnosti. V tomto případě omezuje počet pokusů, které jsou k dispozici pro uhádnutí hodnoty PINu. Pokud se daný počet pokusů vyčerpá, systém PIN se zablokuje. Na odblokování je nutné použít nějaký složitější mechanizmus. Tímto druhým mechanizmem může být mnohem delší PIN nebo osobní kontakt se zákaznickým centrem. [4]

2.4.3 Jednorázová hesla

Jedná se o hesla, která se mění pravidelně, mají z principu omezenou dobu platnosti, typicky několik minut. Z hlediska bezpečnosti útočníkovi odposlechnutí tohoto hesla nepřináší žádnou výhodu, protože takové heslo nelze opětovně použít.[4]

Možnosti generování jednorázových hesel:

- Seznam jednorázových hesel - sdílí se mezi uživatelem a systémem. Každé heslo je možné použít pouze jednou. Hesla mohou být brána ze seznamu postupně, případně je možné vyžadovat zadání dalších doposud platných hesel, nebo použít protokol typu výzva – odpověď. Hlavní nevýhodou je nutnost údržby stejných seznamů hesel na obou stranách;
- Pravidelně aktualizovaná jednorázová hesla - na počátku procesu uživatel sdílí se systémem jedno heslo, jakmile ho uživatel použije, zasílá systému nové heslo šifrované klíčem, které je odvozené z hesla původního. Toto nové heslo je předmětem příštího procesu autentizace, avšak tento způsob je náchylný k chybám při komunikaci.;
- Pravidelně aktualizovaná jednorázová hesla s využitím jednosměrné funkce - v každém autentizačním procesu je zasílán systému výsledek několikanásobné aplikace jednosměrné funkce na heslo, v každém dalším kroku je počet těchto iterací snižován. Kontrolu údajů systém provádí tak, že na poslední předložený hash aplikuje jednosměrnou funkci a výsledek porovnává s předposledním předloženým hashem. Jestliže se tyto výsledky rovnají, autentizace je úspěšná. [4]

2.4.4 Autentizační tokeny

Další možnost je použití autentizačních tokenů. Jsou to zařízení, která mohou uživatelé nosit neustále u sebe a jejichž vlastnictví je nutné pro autentizaci do systému. Tokeny mají buď specifické fyzikální vlastnosti, obsahují tajné informace (např. kvalitní heslo či kryptografický klíč), nebo jsou dokonce schopny provádět některé výpočty. [4]

2.4.5 Karty

Karty jsou asi nejběžnějším autentizačním tokenem. Karty je možno dělit na karty:

- s magnetickým proužkem – magnetický proužek obsahuje normálně neměnnou informaci, kterou lze kdykoliv přepsat,

- čipové karty – jsou složitější než karty s magnetickým proužkem. Karty mohou mít viditelné kontakty nebo mohou komunikovat bezkontaktně pomocí RFID čipu a čtečky vybavené anténou. [4]

2.4.6 Autentizační kalkulátory

Autentizační kalkulátory jsou samostatná technická zařízení vyžadující zvláštní infrastrukturu, kterou nabízí výrobce příslušného kalkulátoru. Samotné kalkulátory jsou založeny na tajemství, které je uloženo v kalkulátoru a na autentizačním serveru, nebo synchronizovaných hodinách. Důležitou vlastností kalkulátorů je způsob komunikace s uživatelem. Rozhraní může být jak klasické – klávesnice a display, tak speciální. Existují např. optická rozhraní, nebo rozhraní využívající infračervený port. [4][2]

2.5 Oblast využití

2.5.1 Finanční instituce

V oblasti bankovnictví a finančních institucí je dnes již běžné, nabízet svým klientům jiné možnosti zprostředkování bankovních a finančních služeb, než jen osobním kontaktem na pobočkách. Toto je způsobeno zejména rozvojem informačních technologií a internetu. Proto banky nabízejí svým klientům elektronické bankovnictví, které má různé formy služeb.

Telefonické bankovnictví – je to služba, která využívá běžné telefonní linky, nebo mobilní telefony. Klient provádí své transakce po zavolání na speciální telefonní číslo banky a komunikuje přímo s telefonním bankéřem, což může být reálná osoba nebo automat. Vstup do systému bude umožněn až po ověření identity, které je většinou ověřováno pomocí uživatelského jména a hesla, nebo PINu. [4]

GSM bankovnictví (GSM Banking - SIM toolkit) – jde o lepší formu bankovnictví u které je vyžadován GSM telefon a to nejlépe s přídavnou funkcí SIM karty. Toto bankovnictví je založeno na aplikaci, která je uložena na kartě. Aplikace zprostředkovává přes intuitivní rozhraní komunikaci mezi klientem prostřednictvím telefonu a bankou. Přístupovým bankovním PINem je zabezpečen přístup ke zprávám banky, či nakládání s účtem. [4]

Internetové a domácí bankovnictví (Internet a Home Banking) – jsou to služby pro manipulaci s účtem prostřednictvím počítače a sítě Internet (nebo prostřednictvím počítače vybaveného modemem a využívajícím veřejnou telefonní síť, toto řešení je však již morálně i technologicky zastaralé a jeho užívání mizí). Z hlediska vybavení se služba dělí na Internet Banking, který může uživatel spravovat svůj účet z kteréhokoliv počítače. Zatímco Home Banking, může uživatel spravovat jen z konkrétního počítače, kde je nainstalován konkrétní software. Možnosti autentizace uživatele, který pracuje prostřednictvím počítače, jsou ovšem mnohem bohatší. Mohou se využívat různé autentizační systémy jako například: uživatelské jméno a heslo, certifikát, čipová karta, SMS kód, autentizační kalkulátor. [4]

2.5.2 E-commerce

Obchodní využívání internetu se nazývá e-commerce, které je možné rozdělit na dvě řešení:

B2B (Business-to-Business)

Pro obchodování mezi obchodními partnery (výměnu dat elektronickou cestou) a firmami jsou určeny aplikace B2B. Zejména se jedná o výměnu informací o obchodních podmínkách (předávání účetních a daňových dokladů atd.) mezi jasně definovanou, zpravidla uzavřenou skupinou uživatelů. V aplikacích B2B jsou procesy obvykle částečně nebo zcela automatizované, jedná se zejména o výměnu dat mezi informačními systémy. A to vyžaduje vysokou úroveň standardizace. Mezi hlavní požadavky patří mimo standardizaci i vysoká míra bezpečnosti přenosu, což zabezpečují technologie založené na moderní kryptografii a certifikátech. Bezpečnostní požadavky lze zjednodušeně charakterizovat, jako dostupnost, důvěrnost, integrita, autentizace a autorizace, nepopiratelnost a přesný čas transakce. [1]

B2C (Business-to-Customers)

Aplikace B2C lze nazvat jako e-shopy, internetové obchody a další. Aplikace B2C je určena pro prodej zboží a služeb konečným spotřebitelům. Proto jsou dány technologické a bezpečnostní požadavky. Důležitým faktem je, že koncovým spotřebitelem je člověk, ne systém. Tudíž je velmi důležité, aby internetové obchody byly přehledné, snadně ovladatelné atd. Toto jsou důležité faktory, které rozhodnou, zda zákazník nakoupí, nebo ne.

Bezpečnostní požadavky zjednodušeně charakterizovat, jako dostupnost, důvěrnost, integrita, autentizace a autorizace, nepopiratelnost, přesný čas transakce.

Rozdíly mezi B2C a B2B jsou hlavně z pohledu přístupu k řešení bezpečnosti. U aplikací B2B mají obě strany zájem ctít dohodnutou úroveň bezpečnosti. B2C je daleko živější. [1]

2.5.3 Státní správa

Elektronizace státní správy a samosprávy je označováno pojmem e-Goverment. V nejlepším případě by se mělo jednat o elektronizaci celého výkonu veřejné moci, a to včetně rozhodovacích procesů. Ministerstvo informatiky definovalo e-goverment jako „transformaci vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií s cílem optimalizovat interní procesy. Jejím cílem je pak rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti a zajištění větší otevřenosti veřejné správy ve vztahu ke svým uživatelům.“ [1]

Mezi hlavní výhody e-Govermentu, jak uvádí Budiš (2008, str. 20), patří:

- rychlost a kvalita služeb občanům,
- jednoduchost, uživatelská přívětivost,
- úřední hodiny pro podání 24 hodin denně, 7 dní v týdnu,
- finanční úspory nákladů na státní správu,
- transparentnost procesů a rozhodování.

Důležitým pojmem v e-govermentu je elektronická podatelna. Elektronickou podatelnu přímo definuje zákon o elektronickém podpisu jako „pracoviště orgánu veřejné moci určené pro příjem a odesílání datových zpráv“. Nařízením vlády ČR č. 495/2004 Sb. je stanovena pro orgány veřejné moci povinnost přijímat a odesílat datové zprávy se zaručenými elektronickými podpisy založenými na kvalifikovaných certifikátech, vydanými akreditovanými poskytovateli certifikačních služeb. K těmto účelům se zřizují elektronické podatelny. Vlastní funkci elektronické podatelny definuje vyhláška o elektronických podatelnách č. 496/2004 Sb. [1]

Dalším důležitým pojmem v e-govermentu je datová schránka. Datová schránka je definována zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, zákon č. 301/2008 Sb..

2.5.4 Další instituce (zdravotnictví, vojenství, věda a výzkum)

- E-health – je v EU momentálně ve stádiu vývoje. Jde hlavně o čipovou kartu zdravotního pojištěnce, elektronické recepty, elektronickou zdravotnickou dokumentaci apod.
- E-procurement – neboli elektronické zadávání veřejných zakázek.
- E-faktura – jedná se o fakturu v elektronické podobě. [2]

2.6 Definice základních pojmů a metod

2.6.1 Elektronický podpis

Elektronický podpis lze chápat, jako veškeré elektronicky vytvořené důkazy o tom, že dokument byl vytvořen konkrétní osobou, nebo konkrétním systémem. Jedná se o důkaz ověření identity podepsané osoby. Takovými důkazy může být podpis vytvořený autentizacím kalkulátorem apod.

Elektronický podpis může sloužit a slouží jako důkaz pravosti dokumentu, za jistých podmínek může být využit jako plnohodnotná náhrada rukou psaného podpisu. Takový podpis se označuje jako zaručený elektronický podpis. Zaručený elektronický podpis je dán nejenom kryptografickými parametry, ale i opatřeními spojenými s bezpečnou generací a správou páru klíčů a zejména legislativními podmínkami státu, ve kterém je potřeba příslušný zaručený podpis uplatnit. [2]

Zaručený elektronický podpis, jak tvrdí Budiš (2008, str. 150), musí splňovat tyto podmínky:

- je jednoznačně spojen s podepisující se osobou,
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,

- je k datové zprávě, ke které se vztahuje, připojen takovým způsoben, že je možno zjistit jakoukoliv následnou změnu dat.

2.6.2 Alternativní metody

Základní metody autentizace uživatelů jsou v zásadě možné provést na základě prokázání:

- *že uživatel něco má* (nějaký předmět/token např. čipovou kartu, mobilní zařízení, autentizací kalkulátor),
- *že uživatel něco ví* (nějaká tajná informace, např. PIN, heslo či přístupová fráze),
- *že uživatel něčím je* (biometrické vlastnosti jako jsou otisky prstů, struktura oční sítnice či duhovky, vzorek DNA atd.). [2]

Všechny tyto metody mají své výhody a nevýhody. Metody, které jsou založeny na principu „něčeho, co daný uživatel zná“, mají hlavní výhodu v tom, že se dají snadno přenášet, či zadávat do počítače. Nevýhodou této metody je zejména tajná informace, která může být lehce zjištěna.

Oproti tomu ono „něco, co daný uživatel má“, představuje hlavně to, že jedná o fyzický objekt (token nebo kalkulátor), který lze jen velmi obtížně zkopírovat a ztráta je snadno zjistitelná. Další výhodou je schopnost uchovávat a zpracovávat náhodné informace s velkou neurčitostí. Jistou nevýhodou může být nekompatibilnost s jinými typy a určitá složitost provedení. K jeho užití musí také existovat příslušné čtecí zařízení nebo ověřovací entita (typicky autentizací server).

U využití „něčeho, čím daný uživatel je“ se typicky jedná o část těla či určitou charakteristiku osoby, která se v čase nemění, nebo se mění jen velmi omezeně. Velkou výhodou této metody je, že nelze nic ztratit nebo zapomenout. Měření biometrických informací bývá obtížné, což je nevýhodou.

Při vzájemné kombinaci těchto metod se zajistí zachování jejich východ a zároveň se eliminují jejich nevýhody. Použití dvou metod se označuje jako dvoufaktorová autentizace a použití všech tří metod se označuje jako třífaktorová autentizace. [4]

Sms autorizace

Transakce pomocí autorizačních SMS představuje jednoduchý a dostupný způsob zabezpečení transakce pomocí kódu zaslaného formou SMS zprávy do mobilního telefonu.

Hardwarové tokeny

Hardwarový token je technické zařízení, které poskytuje bezpečnostní funkce spojené s ukládáním soukromých klíčů, tajných klíčů, sdílených tajemství a jiných aktiv držitele hardwarového klíče. Hardwarový token je propojen s počítačem, který je vybaven příslušným rozhraním. Rozhraním může být: sériový port, USB, SCSII, PCI, PCMCIA apod. Hardwarový klíč zajišťuje funkce, jako generování dvojice veřejného/soukromého klíče, generování podkladů pro žádost o certifikát, vydaný certifikát uloží opět do hardwarového klíče, v případě použití soukromého klíče aplikace vyšle data do hardwarového klíče a hardwarový klíč provede šifrování soukromým klíčem uloženým v hardwarovém klíči.

Hardwarový klíč lze používat jen v prostředí, které je kontrolované samotným uživatelem (např. osobní počítač), nebo v prostředí kontrolovaném správcem aplikace. Nebezpečí hrozí zejména při použití hardwarových klíčů v prostředí kontrolovaném třetí stranou. [2]

Softwarové tokeny (tokeny v mobilních zařízeních)

Softwarový token má podobu aplikace, která musí být nainstalována v zařízení, jehož hardware bude pro výpočty použit. Jsou tedy zpravidla uloženy na stejném zařízení, jako ze kterého probíhá autentizace. Úroveň bezpečnosti, kterou je softwarový token schopen poskytnout je tak přímo závislá na bezpečnosti hostitelského systému, kterým může být jak klasický počítač, tak i notebook nebo smartphone.

Použití tokenu je závislý na zadání správného PINu. Pokud uživatel zadá několikrát po sobě chybný PIN, tak se šifrovací klíče na něm uložené zničí. Softwarový token, ale nemusí být jen prostý soubor nebo šifrovací klíč chráněný heslem, ale může být stejně jako hardwarový token sloužit ke generování jednorázových hesel. Nejrůznější smartphony mohou být vybaveny potřebným softwarem a tím mohou být lehce přeměněny v generátory

jednorázových hesel a pokud autentizace neprobíhá přímo v nich, je možné o nich uvažovat jako o vhodné náhradě klasických hardwarových tokenů.

Výhodou softwarových tokenů je jejich cena. Jsou totiž výrazně levnější než hardwarové tokeny a tak podstatně snižují celkové náklady. Nevýhodou softwarového tokenu je z principu nižší možné zabezpečení, nepřenositelnost, a pokud dojde k poškození počítače, či zařízení může dojít ke ztrátě soukromého klíče. Tato nevýhoda je kompenzována jednak snadnou reaktivací tokenu a dále pak přesunem ověření na samotnou distribuci tajemství (typicky předání inicializačního klíče tokenu formou bezpečné obálky (maileru) uživateli – tento proces je často spojován s ověřením identity uživatele, např. na pobočce).

PKI (Public Key Infrastructure)

PKI je možno definovat jako komplexní systém, který svým uživatelům poskytuje služby v oblasti šifrování pomocí asymetrické kryptografie a služby spojené s digitálními podpisy. Účelem infrastruktury veřejných klíčů je pak hlavně správa jednotlivých soukromých klíčů a certifikátů. PKI v sobě spojuje řadu komponentů – digitální certifikáty, klíče, asymetrickou kryptografii, certifikační autority a aplikace do celkové sítě bezpečnostní architektury. Typická podniková infrastruktura PKI zahrnuje bezpečné vydávání digitálních certifikátu individuálním uživatelům a serverům, integraci s podnikovým adresářem, nástroje pro správu, obnovu, rušení certifikátů, integraci do aplikací a s tím spojené školení, služby a podporu.

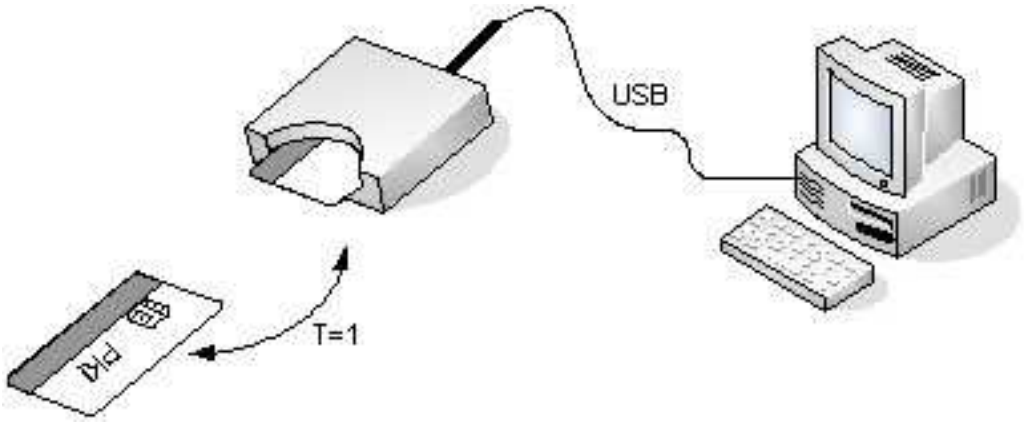
PKI ochraňuje informace několika základními způsoby:

- autentizace přístupu (ověření totožnosti uživatele, PKI nahrazuje snadno uhodnutelná a často ztrácená ID uživatelů a hesla),
- prověření integrity,
- nepopiratelnost transakce pomocí elektronického podpisu, čehož se využívá při styku s úřadem nebo při nákupu přes internet,
- zajištění privátnosti (nepřečtení) zásilky během jejího transportu internetem pomocí vhodné kombinace symetrické a asymetrické šifry.

PKI čipové karty jsou procesorové čipové karty schopné provádět příkazy nejenom symetrické kryptografie, ale i asymetrické kryptografie a často i výpočet otisku. PKI čipové

karty zpravidla mají kryptografické moduly pro urychlení kryptografických operací. PKI čipové karty mohou být jak kontaktní, nebo bezkontaktní. Zejména soukromé klíče určené pro vytváření elektronického podpisu je nutné chránit proti kompromitaci. Jednou z možných cest této ochrany je generování dvojice veřejný/soukromý klíč samotnou PKI čipovou kartou a uložení soukromého klíče do paměťové oblasti karty.

Čtečka čipových karet se označuje jako terminál. Jedná se o zařízení, které zprostředkovává komunikaci s čipovou kartou. Čtečka může být jako samostatné zařízení nebo může být propojena např. s počítačem.



Obrázek 2.1 – Propojení čtečky čipových karet s počítačem[1]

EMV (hardwarový token v kombinaci s platební kartou)

Hlavním úkolem EMV (vytvořené společnostmi Europay International, MasterCard International a Visa International) je zajištění, a to na celosvětové úrovni, interoperability platebních systémů založených na použití kontaktních čipových karet. Bezhotovostní platby, které jsou prováděny pomocí EMV čipových karet a platebních terminálů by měly být v porovnání s použitím klasických karet s magnetickým proužkem bezpečnější.

Standard EMV je popsán ve čtyřech samostatných dokumentech, které specifikují požadavky na čipové karty a platební terminály, na bezpečnost mechanizmů offline autentizace dat a šifrování PINů, generování aplikačních kryptogramů apod.

Offline autentizace dat je prvním bezpečnostním mechanizmem. Offline autentizace dat umožňuje detekovat falešné karty, které jsou vloženy do terminálů. Tento typ autentizace využívá PKI a techniky asymetrické kryptografie. U PKI a techniky asymetrické kryptografie

[1] [online][cit.2011-01-16] Dostupný z WWW:http://itsolutions.siemens.cz/web/topics/main_topic7

je žádoucí existence důvěryhodné certifikační autority, která bude schopna podepisovat veřejné klíče vydavatelů platebních karet.

Dalším bezpečnostním mechanizmem, který přichází na řadu po offline autorizaci dat uložených na čipové kartě je autentizace uživatelů platebních karet. Autentizace může být založena na různých principech, jako je použití klasického podpisu, PINu, nebo na kombinaci podpisu a různých technik ověření PINu.

Po autentizaci uživatelů přichází na řadu automatická analýza rizik, která má na starosti, co nejvíce minimalizovat pravděpodobnost podvodu, a chránit tak všechny účastníky podílející se na dané finanční transakci. Rozhodnutí zda bude transakce přijata, či zamítnuta offline, nebo zda bude vyžadována online autorizace platby vydavatelem karty záviset na výsledku analýzy. Pokud dojde k případné online autorizaci karty, která je založena na symetrické kryptografii, musí být navíc na kartě bezpečně uložen dodatečný tajný klíč, který je sdílen s bankou. Na základě tajného klíče je poté pro každou transakci odvozen dočasný klíč, který je nezbytný pro vytváření MAC (Message Authenication Code) dat příslušné transakce. Poté je dočasný klíč porovnán s klíčem uloženým v bance. Jsou-li oba klíče shodné, pravost karty je potvrzena.

Poměrně široká škála bezpečnostních mechanizmů upřesňuje standard EMV. Z bezpečnostních mechanizmů nejsou všechny povinné, proto závisí bezpečnost celého platebního systému na konkrétní implementaci. V tomto případě se jedná o nalezení vhodného kompromisu mezi cenou, výkonem a bezpečností. [4]

Obrázek 2.2 – Platební karta[2]

[2] [online][cit.2011-01-16]
Dostupný z WWW :http://www.truechance.ws/indexhu.php?page=bankyemboskarty

2.6.3 Životní cyklus certifikátu

V průběhu času prochází certifikát několika fázemi, které tvoří životní cyklus certifikátu.

Životní cyklus certifikátu, jak tvrdí Dostálek (2009, str. 74), se skládá z několika fází:

- vytvoření žádosti o certifikát – vytvoření žádosti může, ale i nemusí předcházet generování párových dat,
- vydání certifikátu a jeho případná publikace,
- platnost certifikátu – poté co byl certifikát vydán, nemusí být automaticky platný,
- vypršení platnosti certifikátu nastane po uplynutí doby uvedené v certifikátu,
- odvolání certifikátu před uplynutím jeho původně deklarované doby platnosti.

Certifikát odvolává certifikační autorita. V okamžiku odvolání certifikátu je tento certifikát zveřejněn v seznamu odvolaných certifikátů (CRL). Ve všech CRL se odvolaný certifikát uvádí po dobu jeho původní platnosti.

Jak tvrdí Dostálek (2009, str. 74), certifikační autorita odvolává certifikát:

- Buď ze svého rozhodnutí, např.:
  - jiný uživatel požádal o certifikaci již certifikovaného veřejného klíče,
  - certifikační autorita zjistila, že údaje v certifikátu nadále nejsou pravdivé.

- Nebo na žádost držitele certifikátu, např.:
  - uživatel si již nepřeje, aby certifikát dále platil z osobních důvodů,
  - byl kompromitován soukromý klíč uživatele,
  - byl zničen soukromý klíč uživatele.

2.6.4 Technologie

V této podkapitole je nutno zmínit technologické zázemí elektronického podpisu. Jak již napovídá samotný název, tyto technologie jsou spjaty s moderním IT, vždy se jedná o

aplikaci **závazných norem** pro danou oblast. Pro ilustraci je zde uveden výčet norem dle vydavatele.

- IEEE
- ISO
- ANSI
- NIST
- IETF
- PKCS
- SECG
- Evropská Unie
- Jiné (ITU, ECBS, apod.)

Typy podpisů

Elektronická značka

Elektronickou značku lze přirovnat k vlastnoručnímu podpisu, elektronickou značku je možno si představit jako otisk razítka. Elektronický podpis a elektronická značka jsou si po technologické stránce velmi podobné, hlavní rozdíl je v legislativní stránce. [5]

Časové razítko

Kvalifikované časové razítko dokazuje existenci dokumentu před časovým okamžikem uvedeným v časovém razítku. Kvalifikovaná časová razítka oproti elektronickému podpisu vydává vždy poskytovatel certifikačních služeb, který disponuje příslušným vybavením, hlavně přesným měřidlem času, které navazuje na koordinovaný světový čas.

Časová razítka jsou nabízena jako služba. Odběratel nejdříve musí podepsat s poskytovatelem certifikačních služeb smlouvu a až poté se vytvoří komunikační kanál. Komunikačním kanálem odběratel posílá tzv. otisky dokumentů, ke kterým poskytovatel certifikačních služeb vydává časová razítka. [5]

Podle zákona č. 227/2000 Sb., o elektronickém podpisu se rozumí časovým razítkem datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

Metody ověření

Postup ověření, vysvětlení pojmů autorizace, autentizace

Postup ověření neboli ověření identity, resp. zadání správné odpovědi na otázku: „jsem skutečně tím, za koho se vydávám?“ Autentizace může být provedena v nejjednodušším případě zadáním hesla. Propracovanější metody autentizace mohou užít techniky elektronického podpisu či zadání zadáním správného kódu autentizačního kalkulátoru.

Nepopiratelnost (neodmítnutelnost) poskytuje důležité záruky, které nabízí zaručený elektronický podpis. Podepsaná osoba nemůže popřít, že podpis byl vytvořen její osobou.

Mezi základní nutnosti při elektronické komunikaci patří zajištění tzv. důvěrnosti. Tím se rozumí zajištění toho, aby se s daným obsahem nemohla seznámit nepovolaná osoba. Požadavek na zajištění důvěrnosti však neznamená, že se obsah zprávy nesmí dostat do rukou nepovolané osoby. Tento podstatně silnější požadavek by se v běžné praxi – například v prostředí dnešního Internetu – dal realizovat jen velmi těžko. U důvěrnosti je nejdůležitější to, aby se případný útočník nemohl seznámit s tím, co má zůstat důvěrné.

Důvěrnost je v praxi zajišťována vhodným zašifrováním daného obsahu. Jedná se o jinou kategorii než elektronický podpis, protože ten důvěrnost nezajišťuje. Avšak u jakéhokoliv elektronického dokumentu je možno zajistit důvěrnost (skrze šifrování) a může být kombinováno s elektronickým podepisováním.

Dalším základním pojmem, se kterým je možno se setkat nejen v souvislosti s elektronickým podpisem, je pojem autorizace. Velmi je tento pojem zaměňován s pojmem autentizace. Autentizace znamená prokazování vlastní identity - jedná se o poskytnutí odpovědi na otázku: „jsem skutečně tím, za koho se vydávám?“ U autorizace to znamená mít práva k určitým úkonům či aktivitám. Konkrétní osoba chce např. získat přístup k nějaké službě, smazat nějaký soubor apod. Otázka je, zda na to má, nebo nemá právo. Autorizací v užším smyslu je udělení konkrétního práva k určitému úkonu. V širším smyslu je autorizace celá správa oprávnění, kterou mají konkrétní subjekty a to včetně přidělování a odnímání těchto práv.

Pravost, resp. autentičnost či autenticita je dalším zajímavým pojmem, se kterým je možné se setkat v souvislosti s e-podpisem. Jednoduše lze „pravost“ pochopit jakože jde o stále „stejný dokument“ a ne o jiný, který by se za něj pouze vydával. Pro ilustraci lze uvést protipříklad: pravost (autenticitu, autentičnost) je možné porušit například tím, že je na

dokumentu něco změněno, nebo je zaměněn s nějakým úplně jiným dokumentem. Elektronický podpis nám pomáhá s určením pravosti dokumentu, a to díky zajištění integrity dokumentu, opatřeného zaručeným elektronickým podpisem: neporušená integrita je důkazem, že dokument nebyl pozměněn či vyměněn. [10]

2.6.5 Vize dalšího využití elektronického ověření identity

Vývoj v oblasti elektronického podpisu jde rovněž směrem, který se nazývá biometrie. Biometrické technologie jsou založeny na měření jedinečných fyziologických vlastností lidského těla (např. otisk prstu, geometrie ruky, rohovkový scan nebo chování člověka (např. dynamika podpisu, vzorek hlasu, typický vzor chůze, držení těla, hlavy), přičemž se jedná o měření automatizovaným způsobem. Některé technologie jsou teprve ve stádiu vývoje, avšak mnohé technologie jsou již relativně vyzrálé a komerčně dostupné (např. otisky prstů, rohovkový scan, otisk dlaně). Systémy založené na fyziologických vlastnostech jsou obvykle spolehlivější a přesnější než systémy založené na chování člověka.

3. Současné a budoucí technologie elektronického podpisu

Změna způsobu zabezpečení internetového bankovnictví je diktována zejména snahou finanční instituce o snížení rizik spojených s rozšířenými útoky, jako jsou např. Phishing, Pharming, MITM, MITB (definice pojmů viz text níže) a na druhé straně snížení nákladů spojených se stávajícím zasíláním autorizačních SMS na jednotlivé transakce. Z toho vyplývá, že základní bezpečnostní metody jako jsou klientské ID a heslo částečně zdokonalené o zasílání autorizačních SMS je nezbytné nahradit jiným způsobem zabezpečení. Jednotlivé metody zabezpečení budou hodnoceny zejména z pohledu bezpečnosti, vhodnosti použití na jednotlivé kanály a uživatelské přívětivosti.

Klientské ID zdokonalené o zasílání autorizačních SMS je možné nahradit různými metodami, například hardwarovým tokenem v kombinaci s platební kartou, PKI čipovou kartou atd. Metod zabezpečení je velké množství, proto je v bakalářské práci řešena pouze metoda autentizačního kalkulátoru Digipass Go 3, Digipass 270 a Digipass for Mobile (což je mobilní bankovnictví založené, také na principu autentizačního kalkulátoru).

V současné době v prostředí internetu a dalších komunikačních sítí existují následující hrozby:

Phishing

Cílem útoku tohoto typu je získání údajů, které uživatel využívá pro přístup k elektronickému bankovnictví. Útok může probíhat několika způsoby. Základní metodou je vylákání přihlašovacích údajů podvržením e-mail zprávy odkazující na stránky, které simulují vzhled aplikace IB, kam klient běžně zadává své autentizační údaje. Klientovy údaje jsou po odeslání zneužity. Takto lze zcizit pouze údaje, které jsou použitelné opakovaně (heslo) a je možné je elektronicky přenést (privátní klíč v souboru). Částečnou obranou proti zneužití ukradených autentizačních údajů představuje vlastnictví předmětu (GRID, TAN) a zcela bezpečné jsou metody založené na dvoufaktorové autentizaci, kde jedním z faktorů je vlastnictví fyzického předmětu (karta, telefon, generátor OTP apod.) a druhý z faktorů je PIN, kterým je použití předmětu umožněno.

Pharming

Útok podobný phishingu vedený za účelem získání autentizačních údajů uživatele. Na rozdíl od phishingu využívá technologických vlastností systému uživatele nebo prostředí internetu, aby přesměroval požadavky uživatele na jiný server, než je původní server elektronického bankovnictví. Tohoto cíle útočníci dosahují mnoha různými technikami. Jako příklad lze uvést modifikaci souboru hosts (používán pro překlad jména serveru na IP adresu) napadením zařízení používaného pro přístup na internet (domácí WiFi AP, na kterém je ponecháno výchozí nastavení od výrobce) apod.

MITM

Man In The Middle - útočník naruší komunikaci tak, že vstoupí do komunikačního spojení a směrem ke klientovi předstírá server a směrem k serveru předstírá klienta. Útočník tak může měnit jak data, která uživatel odesílá na server, tak data, která server odesílá klientovi. Provedení tohoto útoku je ztíženo využitím SSL (HTTPS), kdy je server prohlížečem autentizován. Pokud by byl server podvržen útočníkem je ve většině případů možné tento útok detekovat, protože server může mít nedůvěryhodný certifikát. Odolávání tomuto útoku předpokládá poučeného uživatele, který správně interpretuje hlášení generovaná prohlížečem. Tento typ útoku je relativně těžké provést, protože útočník musí získat přístup k přenosové trase. Druhou možností, jak realizovat útok je modifikace konfigurace síťového připojení na klientské stanici.

MITB

Man In The Browser - tento útok je dokonalejší variantou MITB, kdy útočník nepracuje pouze se síťovou komunikací, ale napadá škodlivým kódem přímo PC uživatele, kde pak může modifikovat chování aplikací dle svých záměrů. V případě internetového bankovnictví může po napadení stanice útočník modifikovat data zadaná uživatelem ještě před tím, než jsou odeslána do banky a dokonce ještě před tím, než je začnou zpracovávat bezpečnostní mechanizmy, které tak útočník dokáže využít ve svůj prospěch. Uživatel, který se stane cílem tohoto útoku, pak nevědomky s využitím všech autentizačních provede transakci ve prospěch útočníka.

3.1 Současná používaná metoda elektronického podpisu v elektronickém bankovnictví

3.1.1 SMS autorizace

Autorizace transakcí pomocí autorizačních SMS je jednoduchý a dostupný způsob zabezpečení pomocí kódu, který je zasílán formou SMS zprávy do mobilního telefonu. Pro využívání SMS autorizace je nutné:

- používat mobilní telefon s funkčním příjmem SMS zpráv – klient,
- aktivovat zasílání autorizačních SMS – poskytovatel. [6]

3.2 Alternativní metody elektronického podpisu

3.2.1 Digipass Go 3

Autentizační kalkulátor Digipass Go 3 zajišťuje bezpečný přístup do vzdálených aplikací a sítí. Je cenově dostupný a uživatelsky přívětivý. Dovoluje rychlé a efektivní zavádění uživatelům.

Digipass Go 3 nevyžaduje zadání PINu, stačí stisknout tlačítko na Digipass Go 3 a vygeneruje One-TimePassword (jednorázové heslo), které uživatel poté použije k přihlášení do aplikace.

Digipass lze kombinovat s různými platformami, včetně počítače, mobilního telefonu a internetovými kiosky. Jeho použití je možné prakticky kdekoliv.

Hesla vygenerovaná Digipass Go 3 mohou být změněna prakticky okamžitě (navíc mají velmi omezenou časovou platnost cca 20 sekund), což znamená, že užití tokenu je vysoce bezpečné. [7]

Obrázek 3.1 – Digipass Go 3[3]

[3][online][cit.2011-03-16]
Dostupný z WWW:http://www.vasco.com/products/digipass/digipass_go_range/digipass_go3.aspx

3.2.2 Digipass 270

Zabezpečení je zákazníkům snadno dostupné odkudkoliv a kdykoliv. Autentizační kalkulátor Digipass 270 nabízí bezpečný a jednoduchý přístup k aplikacím.

Je založený na silné dvou-faktorové autentizaci. K získání přístupu k aplikacím a službám je nutné znát:

- osobní identifikační číslo (PIN),
- mít u sebe Digipass 270.

Poté co se vloží PIN do zařízení, Digipass 270 vygeneruje One-TimePassword. OTP umožňuje bezpečný přístup k aplikacím. Při zadání několika špatných pokusů PIN se Digipass 270 automaticky zablokuje. Kromě již zmíněného OTP (one time password) tento kalkulátor podporuje zadání MAC pro zabezpečení aktivní transakce (tento typ zabezpečení znemožňuje útok typu MITM), případně podporuje challenge–response. Použití metody: pro zabránění odposlechu hesla se logicky nesmí posílat přímo samotné heslo. Proto se používá metoda challenge-response spočívající v tom, že server vytvoří řetězec "výzvu" a pošle ji klientovi (počítači uživatele). Uživatel zadá heslo, ještě v jeho počítači se heslo určitým způsobem zkombinuje s výzvou, z této kombinace se vytvoří hash a ten se pošle serveru. Server pak vezme výzvu, kterou uživateli přidělil, zkombinuje uživatelovo heslo (toto má uloženo např. v databázi) s výzvou, udělá hash a ověří, zda je shodný jako hash, který poslal uživatel. V tomto případě se po síti neposílá heslo, takže ho není možné ani odposlechnout. Je možné získat jen otisk kombinace hesla s výzvou, případně ještě samotnou výzvu.

Funkcionalita podporovaná kalkulátorem je plně customizovatelná, zákazník musí pouze vyplnit parameter sheet pro personalizaci a inicializaci daného zařízení výrobcem. [8]

Obrázek 3.2 – Digipass 270[4]

[4] [online][cit.2011-03-16] Dostupný z WWW: http://www.vasco.com/products/digipass/digipass__e-signature/digipass_250-300_range/digipass_270.aspx

3.2.3 Digipass for Mobile

E-banking a mobilní bankovnictví čelí mnoha nebezpečím. Digipass for Mobile nabízí dvou-faktorovou autentizaci. Toto mobilní bankovnictví je založeno na principu autentizačních kalkulátorů.

Tato metoda je založena na funkci SIM Toolkit, která je naprogramovaná na SIM kartě v mobilním telefonu. SIM Toolkit nabízí možnost rychle zadat požadovanou operaci nebo zjistit potřebné informace, bez nutnosti použití specializovaného zařízení, prakticky odkudkoli.

Výhodou této metody je, že není zapotřebí žádného speciálního zařízení, stačí jen mobilní telefon podporující SIM Toolkit. V případě Digipass for Mobile je podporována stejná množina služeb jako v případě DP 270 čili:

- OTP
- MAC
- Challenge – response.

Digipass for Mobile je rovněž plně customizovatelný (provádí se zákaznickou úpravou xml souboru). [9]

3.2.4 Srovnání metod autentizace z hlediska bezpečnosti

Metoda	Phishing	Pharming	MITM	MITB
SMS OTP	ANO	ANO	ČÁST.	ČÁST.
Digipass Go 3	ANO	ANO	ČÁST.	ČÁST.
Digipass 270	ANO	ANO	ANO	ANO
Digipass for Mobile	ANO	ANO	ANO	ANO

Tabulka 3.1 – Srovnání metod z hlediska bezpečnosti
ZDROJ: vlastní zpracování

Kritéria:

- ANO – metoda účinně zabrání uvedené hrozbě,
- ČÁST. – metoda částečně odolává uvedené hrozbě,
- NE – metoda nedokáže odolat útoku vedenému s využitím uvedené hrozby.

3.2.5 Význam bezpečnostních atributů v kontextu provádění transakcí v Internet bankingu

Bezpečnostní atributy jsou vybrány tak, aby bylo dostatečně zabezpečeno přihlášení do Internet bankingu, odeslání platebního příkazu a pasivního prohlížení informací.

- identifikace – pomocí metody lze realizovat identifikaci držitele v systému;
- autentizace – pomocí metody lze ověřit, že uvedená identita opravdu přísluší tomu, kdo s metodou pracuje;
- autorizace – opětovné ověření identity společně s požadavkem na provedení transakce;
- integrita – metoda zajišťuje možnost prokázat, že data, jak dorazila do bankovního systému, nebyla během přenosu změněna;
- důvěrnost – metoda dokáže zajistit ochranu přenášených dat před neoprávněným čtením;
- neodmítnutelnost – pomocí metody je možno prokázat, že klient je původcem zprávy tak, že ani klient nemůže obvinit banku, že si důkazy vygenerovala sama;
- opora v legislativě – většina bezpečnostních metod svou právní vymahatelnost opírá o dvoustranný smluvní vztah. Některé z metod však mají oporu přímo v legislativě a při vymáhání je možné se opřít o další pilíř.

Metoda	Identifikace	Autentizace	Autorizace	Integrita	Důvěryhodnost	Neodmítnutelnost	Opora v legislativě
SMS OTP	ANO	ANO	ANO	ČÁST.	NE	NE	NE
Digipass Go 3	ANO	ANO	ANO	ČÁST.	NE	NE	NE
Digipass 270	ANO	ANO	ANO	ANO	ANO	ANO	NE
Digipass for Mobile	ANO	ANO	ANO	ANO	ANO	ANO	NE

Tabulka 3.2 - Bezpečnostní atributy zajišťované jednotlivými aut. metodami
ZDROJ: vlastní zpracování

Kritéria:

- ANO - daná metoda poskytuje možnosti k ochraně daného bezpečnostního atributu komunikace;
- ČÁST. - daná metoda dokáže ochránit konkrétní atribut za splnění určitých předpokladů;
- NE - s využitím dané metody nelze ochránit konkrétní atribut elektronické komunikace.

SMS OTP poskytuje druhý nezávislý kanál pro ověření transakcí, které jsou odesílány potenciálně kompromitovaným kanálem přes PC. Kromě autentizace a autorizace transakce poskytují částečně rovněž možnost ověřit integritu dat tím, že uživatel porovná, jaká data zamýšlel odeslat s daty, která mu přišla v SMS zprávě. Tato možnost je realizovatelná pouze pro malé objemy dat (typicky jednorázový platební příkaz).

3.2.6 Použitelnost metod autentizace pro různé obslužné kanály

Metoda	IB	Telefon	Pobočka
SMS OTP	ANO	ANO	ANO
Digipass Go 3	ANO	ANO	ANO
Digipass 270	ANO	ANO	ANO
Digipass for Mobile	ANO	ANO	ANO

Tabulka 3.3 - Použitelnost metod v jednotlivých kanálech (autentizace)
ZDROJ: vlastní zpracování

V internetovém bankovnictví je možné používat kteroukoliv z porovnávaných metod.

Kritéria:

- ANO – metoda lze v daném kanálu využít,
- NE – metody nelze z technických nebo bezpečnostních důvodů použít.

3.2.7 Porovnání vlastností metod z pohledu uživatele

Metoda	Instalace klientské komponenty	HW u klienta
SMS OTP	NE	ČÁST.
Digipass Go 3	NE	ČÁST.
Digipass 270	NE	ČÁST.
Digipass for Mobile	NE	ČÁST.

Tabulka 3.4 – Použitelnost vlastností metod
ZDROJ: vlastní zpracování

Kritéria:

- Instalace klientské komponenty
  - ANO – je nutné instalovat klientskou komponentu,
  - NE – není nutné instalovat klientskou komponentu.
- HW u klienta
  - ANO – klient musí být vybaven HW a ovladač tohoto HW instalován na počítač,
  - ČÁST. – klient musí být vybaven HW, ale bez nutnosti instalovat další sw komponenty; alternativně toto hodnocení znamená, že klient může být vybaven HW či jiný neaktivním předmětem pro některé varianty metody (vylepšené heslo – např. papírová GRID karta),
  - NE – není třeba, aby klient používal žádný pro metodu specifický HW.

3.2.8 Přehled zařízení z pohledu uživatelského komfortu

Metoda	Komfort použití
SMS OTP	ANO
Digipass Go 3	NE
Digipass 270	NE
Digipass for Mobile	ANO

Tabulka 3.5 Přehled zařízení z pohledu uživatelského komfortu
ZDROJ: vlastní zpracování

Kritéria:

- ANO - případné použití metody nevyžaduje další specifické zařízení,
- NE - vyžaduje použití dalšího specifického zařízení.

V této kapitole jsem se zabývala srovnáním metod SMS OTP, Digipass Go 3, Digipass 270 a Digipass for Mobile z různých hledisek.

Na základě srovnávací tabulky (3.1) je jasné, že nejbezpečnější metody jsou Digipass 270 a Digipass for Mobile, protože obě tyto metody jsou schopny účinně zabránit uvedeným hrozbám. Oproti metodám SMS OTP a Digipass Go 3, které dokážou zabránit útokům Phishing, Pharming, ale útokům MITM a MITP odolají jen částečně.

Z tabulky (3.2) vyplývá, že všechny sledované metody poskytují možnost k ochraně bezpečnostních atributů komunikace, jako jsou identifikace, autentizace a autorizace. Integritu zajišťují pouze metody Digipass 270 a Digipass for Mobile. Důvěryhodnost a neodmítnutelnost poskytuje jen metoda Digipass 270 a Digipass for Mobile. Oporu v legislativě nemá žádná z řešených metod.

Použitelnost pro různé obslužné kanály (Internetové bankovnictví, telefon, pobočka), která byla řešena v tabulce (3.3) je vhodná pro všechny řešené metody.

Podle tabulky (3.4) není nutné u žádné z metod instalovat klientskou komponentu. Klient musí být pouze vybaven HW.

SMS OTP a Digipass for Mobile jsou z pohledu uživatelského komfortu nejméně náročné, při použití nevyžadují žádné specifické zařízení oproti Digipass Go 3 a Digipass 270.

V závěru této kapitoly je možné zhodnotit, jako nejvhodnější metodu Digipass for mobile, případně Digipass 270.

4. Zpracování modelu na jiné metody autentizace a autorizace

Cílem této části bakalářské práce je zmapovat a porovnat aspekty současného řešení a navrhovaných alternativních metod v oblastech:

- Obchodní model
- Finanční model
- Omezení
- Modelový Business Case

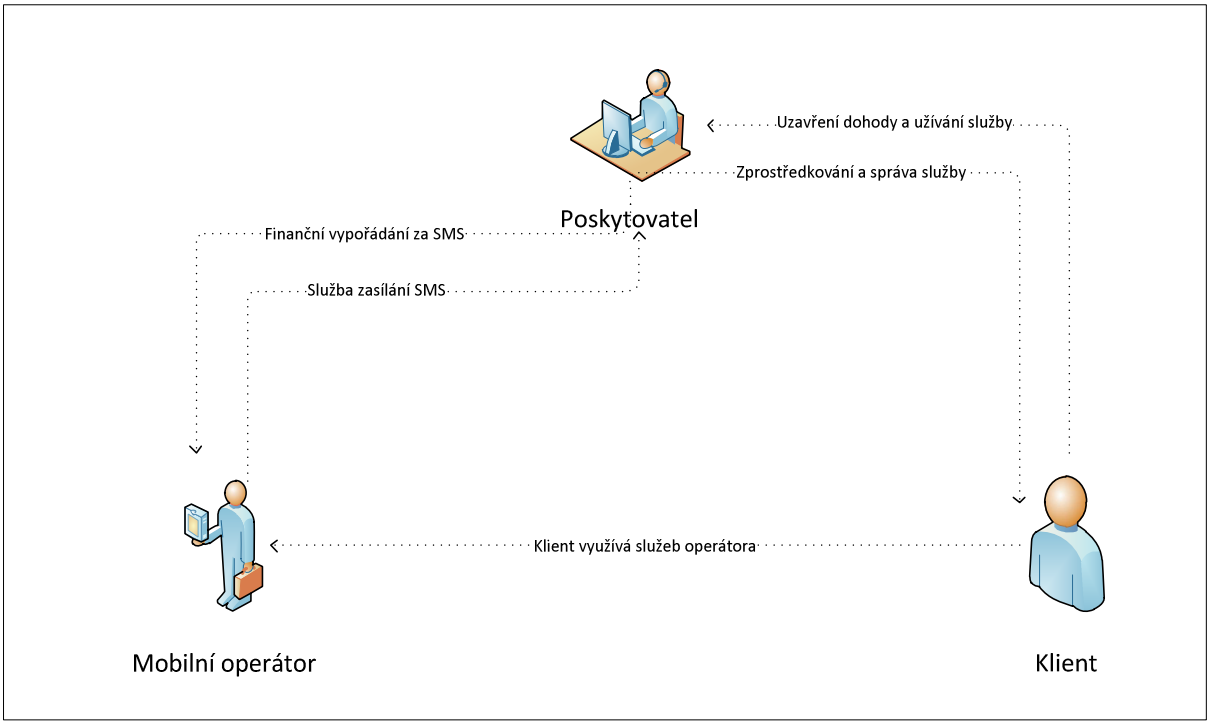
Obchodní strategie

Motivací pro porovnání možností použití alternativních metod je především snaha finanční instituce o zvýšení bezpečnosti používaných autentizačních a autorizačních metod a rovněž v maximální možné míře snížení nákladů na jejich použití.

4.1 Obchodní model

Obchodní model znázorňuje obecné vztahy mezi poskytovatelem služby, zákazníky a dalšími subjekty, jež jsou nezbytnou součástí celého procesu poskytování jednotlivé metody zabezpečení. Níže uvedené schémata objasňují základní pohled na vztahy mezi výše uvedenými subjekty.

4.1.1 Současný stav - Model pro metodu SMS autorizace



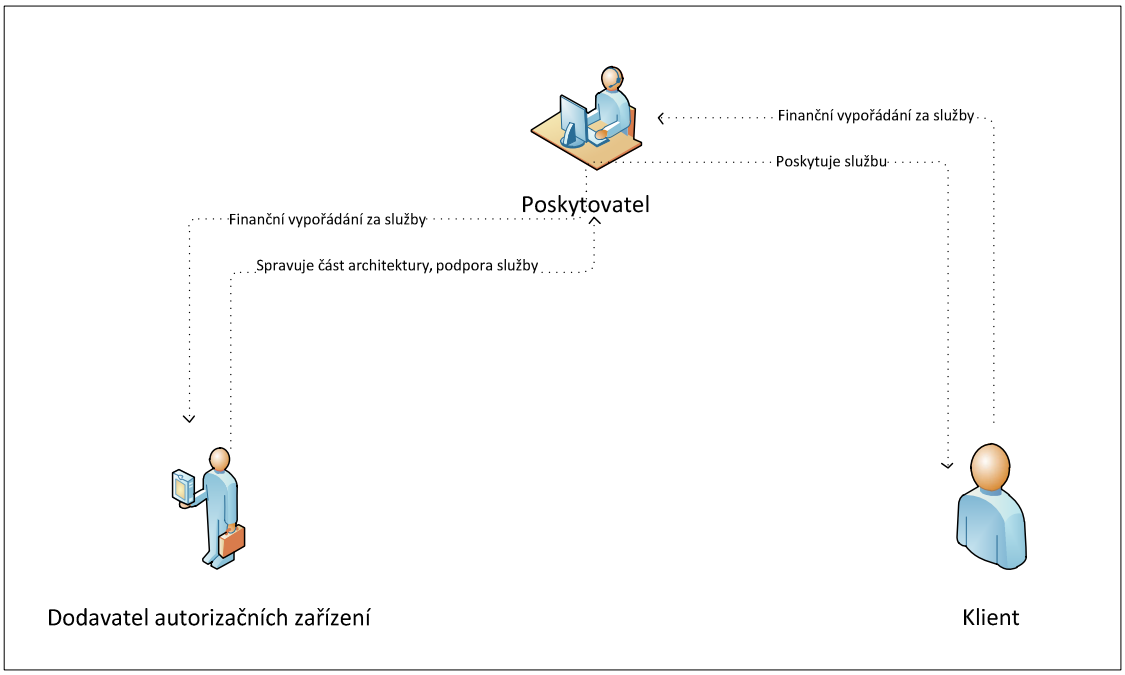
Obrázek 4.1 – Znázornění obchodního modelu pro metodu SMS autorizace
ZDROJ: interní materiály A&&L soft, s.r.o.

Do modelu vstupují 3 subjekty: Poskytovatel služby, Mobilní operátor, Klient

- **Vztah Poskytovatel – Klient**: Poskytovatel ve vtahu ke klientovi zprostředkovává služby, za které klient poskytovateli platí.
- **Vztah Poskytovatel – Mobilní operátor:** Mobilní operátor poskytuje poskytovateli služby automatického odesílání SMS, za což se operátor s poskytovatelem finančně vypořádává.
- **Vztah Mobilní operátor – Klient:** Klient využívá služeb operátora prostřednictví poskytovatele.

4.1.2 Navrhovaný stav - Model pro metodu autentizace (autorizace) HW a SW token

Obchodní model pro nově navrhované metody Digipass GO3, Digipass 270, Digipass for Mobile je analogický.



Obrázek 4.2 – Znázornění obchodního modelu pro metodu HW a SW token Vasco
Zdroj: interní materiály A&&L soft, s.r.o.

Do modelu vstupují 3 subjekty: Poskytovatel služby, Dodavatel autorizačních zařízení, Klient.

- **Vztah Dodavatel autorizačních zařízení – Poskytovatel služby:** Dodavatel autorizačních zařízení spravuje pro poskytovatele služby část architektury, taktéž poskytuje podporu pro služby, za což se poskytovatel služby s dodavatelem služby finančně vypořádává.
- **Vztah Poskytovatel služby – Klient:** Poskytovatel služby poskytuje klientovi službu autentizačního kalkulátoru, za kterou se klient s poskytovatelem služby finančně vypořádává.

Na základě porovnání obchodního modelu stávající metody a metody nově navržené je možno identifkovat, že zavedením kterékoliv z nově navržených metod eliminujeme nutnost existence jakéhokoliv obchodního vztahu mezi klientem a řekněme participantem na celkovém řešení v tomto případu na mobilním operátorovi.

4.2 Finanční model

Řešení současného finančního modelu je zaměřen na mapování současných nákladů finanční instituce (banky) pro úhradu plateb za poskytované služby zabezpečení dle počtu

provedených transakcí u metody SMS autorizace a rovněž předpokládaných nákladů na použití nově navrhovaných metod.

Uvedené hodnoty nejsou reálné především v oblasti ceny za jednotku SMS a ceny za jednotku autentizačních kalkulátorů, byly však získány z interních materiálů A&&L soft, s.r.o., kdy došlo k poměrné úpravě jejich výše ve všech případech tak, aby nedošlo ke zkreslení výsledků v porovnání jednotlivých zkoumaných metod. Vypočtené hodnoty jsou dále použity v následující kapitole Business Case.

V níže uvedeném modelu je předpokládán 10% růst počtu klientů v následujícím období pěti let.

Pro uvedený výpočet byl, použit hypotetický případ s následujícími parametry:

Rok	Počet klientů	Prům. počet transakcí klient/rok	Celkový počet transakcí/rok
2012	150 000	120	18 000 000
2013	165 000	120	19 800 000
2014	181 500	120	21 780 000
2015	199 650	120	23 958 000
2016	219 615	120	26 353 800

Tabulka 4.1 – Růst počtu klientů v následujících letech
ZDROJ: vlastní zpracování

4.2.1 Současný stav - Finanční model metody SMS autorizace

	Kalkulační vzorec	Cena za jednotku	2012	2013	2014	2015	2016
Transakce (odeslaná SMS)	Počet zaslaných SMS*cena SMS	0,4 Kč	7 200 000 Kč	7 920 000 Kč	8 712 000 Kč	9 583 200 Kč	10 541 520 Kč
Inicializační náklady		0 Kč	0 Kč	0 Kč	0 Kč	0 Kč	0 Kč

Tabulka 4.2 – Finanční model metody SMS autorizace
ZDROJ: vlastní zpracování

Na základě uzavřených smluv s mobilními operátory se cena SMS v jednotlivých letech nemění.

U metody SMS autorizace (tab. 4.2) nevznikají finanční instituci žádné inicializační náklady, neboť tato metoda byla zavedena již v předchozích letech. Nákladem je tedy jen cena za transakci, což je cena za zaslanou SMS.

4.2.2 Navrhovaný stav - Finanční model metody autentizační kalkulátor Digipass GO3

	Kalkulační vzorec	Cena za jednotku	2012	2013	2014	2015	2016
Transakce (provedena prostřednictví kalkulátoru)		0 Kč	0 Kč	0 Kč	0 Kč	0 Kč	0 Kč
Inicializační náklady (nákup zařízení)	Cena zařízení *přírůstek klientů	75 Kč	11 250 000 Kč	1 125 000 Kč	1 237 500 Kč	1 361 250 Kč	1 497 375 Kč

Tabulka 4.3 – Finanční model metody Digipass Go 3
ZDROJ: vlastní zpracování

4.2.3 Navrhovaný stav - Finanční model metody autentizační kalkulátor Digipass for Mobile

	Kalkulační vzorec	Cena za jednotku	2012	2013	2014	2015	2016
Transakce (provedena prostřednictví kalkulátoru)		0 Kč	0 Kč	0 Kč	0 Kč	0 Kč	0 Kč
Inicializační náklady (nákup zařízení)	Cena zařízení*přírůstek klientů	115 Kč	17 250 000 Kč	1 725 000 Kč	1 897 500 Kč	2 087 250 Kč	2 295 975 Kč

Tabulka 4.4 – Finanční model metody Digipass for Mobile
ZDROJ: vlastní zpracování

4.2.4 Navrhovaný stav - Finanční model metody autentizační kalkulátor Digipass 270

	Kalkulační vzorec	Cena za jednotku	2012	2013	2014	2015	2016
Transakce (provedena prostřednictví kalkulátoru)		0 Kč	0 Kč	0 Kč	0 Kč	0 Kč	0 Kč
Inicializační náklady (nákup zařízení)	Cena zařízení*přírůstek klientů	145 Kč	21 750 000 Kč	2 175 000 Kč	2 392 500 Kč	2 631 750 Kč	2 894 925 Kč

Tabulka 4.5 – Finanční model metody Digipass 270
ZDROJ: vlastní zpracování

Navrhované metody Digipass Go 3(tab. 4.3), Digipass for Mobile (tab. 4.4) a Digipass 270 (tab. 4.5) nemají žádné náklady na provedení transakce prostřednictvím kalkulátoru. Do nákladů vstupuje cena za nákup jednotlivých zařízení. V roce 2012 jsou inicializační náklady nejvyšší a to z důvodu převedení stávajících klientů na nové metody. V dalších letech jsou řešeny inicializační náklady na nákup zařízení 10% přírůstku klientů.

Po vyhodnocení požadavků je možno konstatovat, že v rámci nabízeného řešení žádná omezení vyplývající ze zavedení, implementace či používání navrženého řešení nejsou evidována.

4.3 Business Case

Pro vyhodnocení ekonomického aspektu nasazení nových metod zabezpečení byl vypracován Business Case ve srovnání staré a nových metod autorizace, který mapuje danou situaci ze základního pohledu na předpokládané investiční a operační náklady. Dále uvedené hodnoty byly použity z kapitoly finanční model a další byly získány z interních materiálů A&&L soft, s.r.o., která má zkušenosti s obdobnými projekty. Dané hodnoty jsou upraveny tak, aby výsledek nebyl zkreslován.

Operační náklady - zahrnují předpokládané náklady na provoz systému pro podporu nových autentizačních metod, včetně nákladů na transakci v případě metody SMS.

Investiční náklady - zahrnují předpokládané náklady na pořízení systému pro podporu nových autentizačních metod a nákup nutného klientského hardware, software.

Výnosy - představují primárně ušetřené náklady za autorizační SMS, které se zavedením nových metod zabezpečení nebudou klientům zasílány.

Při odhadu operačních nákladů byl jako v kapitole finanční model uvažován roční 10% nárůst počtu klientů. U nákladů na provoz systému se předpokládá 5% nárůst. Dále je kalkulován předpokládaný fixní výdaj (update SW a HW) ve výši 1 500 000 Kč každý lichý rok analogicky pro všechny navrhované metody.

4.3.1 Business Case – metoda SMS x Digipass GO 3

	2012	2013	2014	2015	2016
Náklady metoda SMS	**13 200 000 Kč**	**15 720 000 Kč**	**15 327 000 Kč**	**18 028 950 Kč**	**17 834 558 Kč**
Investiční náklady	-	1 500 000 Kč	-	1 500 000 Kč	0 Kč
Operační náklady	13 200 000 Kč	14 220 000 Kč	15 327 000 Kč	16 528 950 Kč	17 834 558 Kč
Provoz systému	6 000 000 Kč	6 300 000 Kč	6 615 000 Kč	6 945 750 Kč	7 293 038 Kč
Náklady na SMS	7 200 000 Kč	7 920 000 Kč	8 712 000 Kč	9 583 200 Kč	10 541 520 Kč
Náklady metoda Digipass Go 3	**20 250 000 Kč**	**8 925 000 Kč**	**7 852 500 Kč**	**9 807 000 Kč**	**8 790 413 Kč**
Investiční náklady - nákup koncových zařízení	11 250 000 Kč	2 625 000 Kč	1 237 500 Kč	2 861 250 Kč	1 497 375 Kč
Investiční náklady – Software pro podporu nových zařízení	3 000 000 Kč	-	-	-	-
Operační náklady	6 000 000 Kč	6 300 000 Kč	6 615 000 Kč	6 945 750 Kč	7 293 038 Kč
Provoz systému	6 000 000 Kč	6 300 000 Kč	6 615 000 Kč	6 945 750 Kč	7 293 038 Kč
Úspora nákladů	**-7 050 000 Kč**	**6 795 000 Kč**	**7 474 500 Kč**	**8 221 950 Kč**	**9 044 145 Kč**

Tabulka 4.6 – Metoda SMS x Digipass GO 3

ZDROJ: vlastní zpracování

Úspora nákladů metody Digipass Go 3 vůči metodě SMS je za pět let 24 485 595 Kč.

4.3.2 Business Case – metoda SMS x Digipass for Mobile

	2012	2013	2014	2015	2016
Náklady metoda SMS	**13 200 000 Kč**	**15 720 000 Kč**	**15 327 000 Kč**	**18 028 950 Kč**	**17 834 558 Kč**
Investiční náklady	-	1 500 000 Kč	-	1 500 000 Kč	-
Operační náklady	13 200 000 Kč	14 220 000 Kč	15 327 000 Kč	16 528 950 Kč	17 834 558 Kč
Provoz systému	6 000 000 Kč	6 300 000 Kč	6 615 000 Kč	6 945 750 Kč	7 293 038 Kč
Náklady na SMS	7 200 000 Kč	7 920 000 Kč	8 712 000 Kč	9 583 200 Kč	10 541 520 Kč
Náklady metoda Digipass for Mobile	**26 250 000 Kč**	**9 525 000 Kč**	**8 512 500 Kč**	**10 533 000 Kč**	**9 589 013 Kč**
Investiční náklady - nákup koncových zařízení	17 250 000 Kč	3 225 000 Kč	1 897 500 Kč	3 587 250 Kč	2 295 975 Kč
Investiční náklady – Software pro podporu nových zařízení	3 000 000 Kč	-	-	-	-
Operační náklady	6 000 000 Kč	6 300 000 Kč	6 615 000 Kč	6 945 750 Kč	7 293 038 Kč
Provoz systému	6 000 000 Kč	6 300 000 Kč	6 615 000 Kč	6 945 750 Kč	7 293 038 Kč
Úspora nákladů	**-13 050 000 Kč**	**6 195 000 Kč**	**6 814 500 Kč**	**7 495 950 Kč**	**8 245 545 Kč**

Tabulka 4.7 - Metoda SMS x Digipass for Mobile
ZDROJ: vlastní zpracování

Úspora nákladů metody Digipass for Mobile za pět let oproti metodě SMS je 15 700 995 Kč.

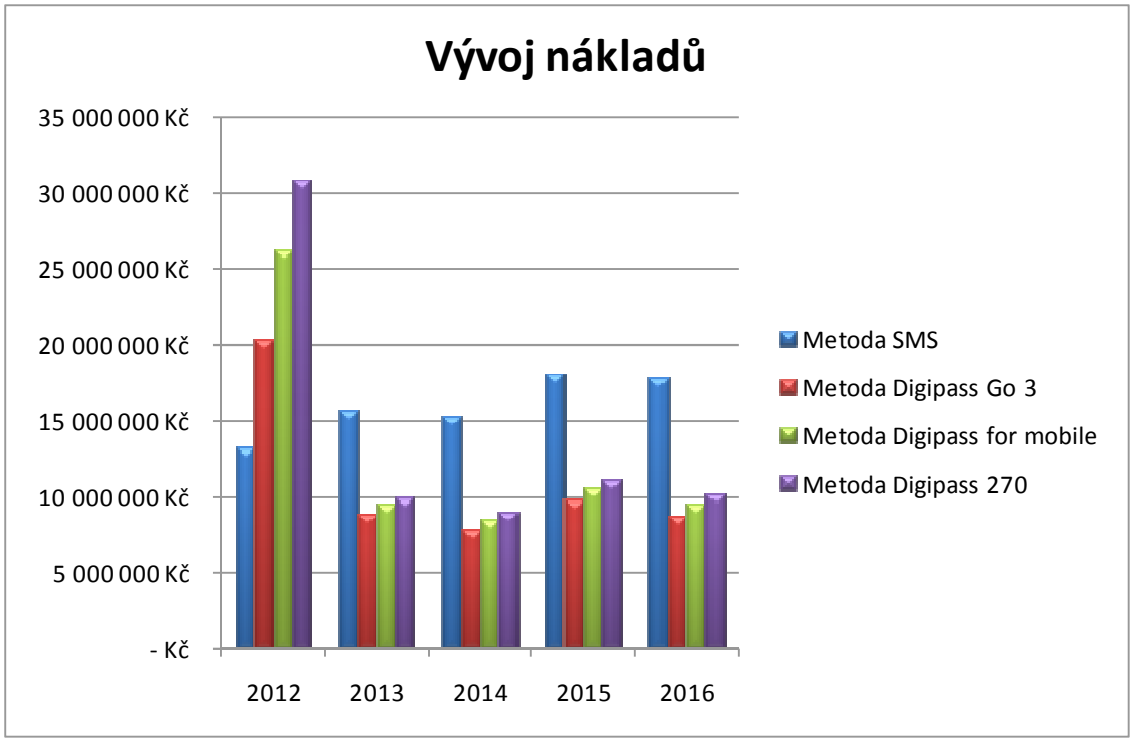
4.3.3 Business Case – metoda SMS x Digipass 270

	2012	2013	2014	2015	2016
Náklady metoda SMS	**13 200 000 Kč**	**15 720 000 Kč**	**15 327 000 Kč**	**18 028 950 Kč**	**17 834 558 Kč**
Investiční náklady	-	1 500 000 Kč	-	1 500 000 Kč	-
Operační náklady	13 200 000 Kč	14 220 000 Kč	15 327 000 Kč	16 528 950 Kč	17 834 558 Kč
Provoz systému	6 000 000 Kč	6 300 000 Kč	6 615 000 Kč	6 945 750 Kč	7 293 038 Kč
Náklady na SMS	7 200 000 Kč	7 920 000 Kč	8 712 000 Kč	9 583 200 Kč	10 541 520 Kč
Náklady metoda Digipass 270	**30 750 000 Kč**	**9 975 000 Kč**	**9 007 500 Kč**	**11 077 500 Kč**	**10 187 963 Kč**
Investiční náklady - nákup koncových zařízení	21 750 000 Kč	3 675 000 Kč	2 392 500 Kč	4 131 750 Kč	2 894 925 Kč
Investiční náklady – Software pro podporu nových zařízení	3 000 000 Kč	-	-	-	-
Operační náklady	6 000 000 Kč	6 300 000 Kč	6 615 000 Kč	6 945 750 Kč	7 293 038 Kč
Provoz systému	6 000 000 Kč	6 300 000 Kč	6 615 000 Kč	6 945 750 Kč	7 293 038 Kč
Úspora nákladů	**-17 050 000 Kč**	**5 745 000 Kč**	**6 319 500 Kč**	**6 951 450 Kč**	**7 646 595 Kč**

Tabulka 4.8 - Metoda SMS x Digipass 270
ZDROJ: vlastní zpracování

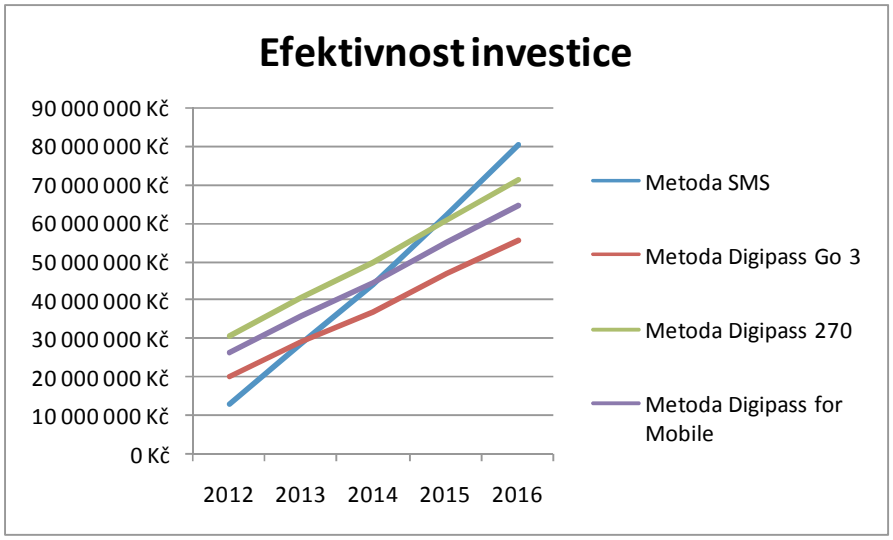
U metody Digipass 270 je úspora nákladů vůči metodě SMS ve výši 9 612 545 Kč za období pěti let.

Z Business Case, které jsou aplikovány na porovnání nákladů metody SMS a metod Digipass Go 3 (tab. 4.6), Digipass for Mobile (tab. 4.7), Digipass 270 (tab. 4.8) vyplývá, že všechny tyto metody mají v roce zavedení vyšší náklady než již zavedená metoda SMS, což je způsobeno převedením stávajících klientů na nově řešené metody a počátečními investičními náklady na software pro podporu nových metod. V dalších letech do investičních nákladů vstupují jen náklady na nákup koncových zařízení pro roční přírůstek nových klientů. Z toho vyplývá, že stávající metoda SMS je nevýhodná a to z důvodu vysokých nákladů na zasílání autorizačních SMS svým klientům. Vývoj nákladů daných metod v jednotlivých letech je zobrazen v grafu (4.1).



Graf 4.1 – Vývoj nákladů
ZDROJ: vlastní zpracování

Efektivností investice je myšlen rok, kdy náklady na nově navržené metody budou menší, než náklady na metodu SMS. Graf (4.2) zobrazuje průniky nově navržených metod se starou metodou SMS. Tyto průniky ukazují, ve kterém roce se stala daná metoda efektivnější než metoda SMS, resp. kdy náklady na nově navržené metody budou nižší než náklady na metodu SMS. Graf (4.2) vychází z celkových nákladů řešených metod v jednotlivých letech.



Graf 4.2 – Efektivnost investice
ZDROJ: vlastní zpracování

Tabulka (4.9) zobrazuje, ve kterém roce budou náklady nově navržených metod Digipass Go 3, Digipass 270 a Digipass for Mobile nižší než náklady na metodu SMS.

	Efektivnost investice (rok)
Digipass Go 3	2
Digipass 270	3
Digipass for Mobile	4

Tabulka 4.9 – Efektivnost investice
ZDROJ: vlastní zpracování

Hodnotící tabulka (4.10) je vypracována tak, bylo možné subjektivně klasifikovat „kvalitu“ jednotlivých zařízení známkou 1-5, a to z hlediska:

- efektivnosti investice,
- uživatelské přívětivosti,
- bezpečnosti (přičemž bezpečnost má při výpočtu průměru váhu 1,5 oproti ostatním kritériím).

Typ zařízení	Efektivnost investice	Uživatelská přívětivost	Bezpečnost	Bezpečnost (přepočtený	Průměrné hodnocení
Digipass GO 3	1	1	3	4,5	2,17
Digipass for Mobile	2	1,5	1	1,5	1,67
Digipass 270	3	1	1	1,5	1,83

Tabulka 4.10 – Hodnotící tabulka
ZDROJ: vlastní zpracování

Z hodnotící tabulky (4.10) je zřejmé, že podle zadaných kritérií vychází, jako nejvhodnější metody Digipass for Mobile a Digipass 270.

Vyhodnocení:

Hlavním cílem této části bakalářské práce bylo porovnání současné metody SMS autorizace s navrhovanými metodami Digipass Go 3, Digipass for Mobile a Digipass 270 a to z hlediska nákladů, efektivnosti investice. Obchodní model znázorňuje vztahy mezi poskytovatelem služby, zákazníky a dalšími subjekty. Ve finančním modelu byly zhodnoceny současné náklady na metodu SMS a předpokládané náklady na nově navržené metody. Pro vyhodnocení ekonomického aspektu nových metod zabezpečení byl vypracován Business Case, který byl srovnáván se starou metodou. Dále byla řešena efektivnost investice a na závěr byla vypracována hodnotící tabulka, z které je možno určit metodu, která bude nejvhodnější, jak pro danou finanční instituci, tak i pro klienty.

Za nejvhodnější metody lze považovat autentizací kalkulátory Digipass for Mobile a Digipass 270. Tyto metody jsou z hlediska bezpečnosti vhodnější pro Internetové bankovnictví oproti SMS autorizace. Pro klienty jsou obě tyto metody pro použití sice trochu složitější než metoda SMS, ale bezpečnost převažuje před tímto hlediskem. Z pohledu finanční instituce jsou obě metody lepším řešením, protože se výrazně sníží náklady.

5. Závěr

Elektronický podpis je významný ve všech oblastech svého použití, zejména však v oblasti bankovnictví. V dnešní době se často využívá internetové bankovnictví, a to zejména z důvodu úspory času i ceny za elektronické transakce. Přes internetové bankovnictví se lze dostat ke svým zůstatkům na účtu a je možné provádět různé transakce apod. Provádění internetového bankovnictví není určitě levnou záležitostí hlavně pro banky, protože je nutné investovat do stále nových metod autentizace a zajištění bezpečnosti této metody. Proto jsem se ve své bakalářské práci zabývala zejména pohledem finanční instituce na bezpečnost a na náklady za využívání internetového bankovnictví svými klienty. Finanční instituce musí zohlednit i uživatelskou přívětivost internetového bankovnictví, proto je v bakalářské práci řešen i tento faktor.

Ve své práci jsem se zabývala problematikou elektronického podpisu, definovala pojem elektronický podpis, zkoumala jsem možné případy jeho užití v různých oblastech lidské činnosti (finančnictví, obchod, státní správa) a kontext této metody z pohledu platné legislativy. Rovněž jsem zmínila důvody vzniku a užití alternativních metod pro podpis či autorizaci v prostředí bankovních aplikací – internet banking.

Dále jsem se zabývala srovnáním staré metody a nově navržených metod z různých hledisek, jako je bezpečnost zařízení, použitelnost metod pro různé obslužné kanály, vlastností metod z pohledu uživatele a z pohledu uživatelského komfortu. Na základě těchto hledisek vyšly jako nejvhodnější metody Digipass for Mobile a Digipass 270.

V další kapitole jsem zmapovala a porovnala aspekty současného řešení a navrhovaných řešení pomocí obchodního modelu, finančního modelu a Business Case. Dále byla brána v potaz efektivnost daných investic. Po vyhodnocení efektivnosti investice, uživatelské přívětivosti a bezpečnosti doporučuji jako výhodné pro bankovní instituci užití Digipass 270 a Digipass for Mobile. Metody Digipass 270 a Digipass for Mobile jsou vhodné zejména z důvodů vysoké bezpečnosti autentizace.

Seznam použité literatury:

[1] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi*. 1. vyd. Olomouc: ANAG, 2008. 157 s. ISBN 978-80-7263-465-1.

[2] DOSTÁLEK, L.; VOHNOUTOVÁ, M. *Velký průvodce infrastrukturou PKI*. 2. vyd. Brno: Computer Press, 2009. 542 s. ISBN 978-80-251-2619-6.

[4] LIDINSKÝ, V. a kol. *eGovernment bezpečně.* 1. vyd. Praha: Grada Publishing, 2008. 160 s, ISBN 978-80-247-2462-1.

[3]MATIÁŠ, V.; KRHOVJÁK, J. *Autorizace elektronických transakcí a autentizace dat uživatelů.* 1. yyd. Brno: Masarykova univerzita, 2007. 125 s. ISBN 978-80-210-4556-9.

[5] STÁŇA, J. *Moderní administrativa ve veřejné správě*. 1. vyd. Praha: Institut pro místní správu Praha, 2010. 123 s. ISBN 978-80-86976-20-4.

Seznam internetových zdrojů:

[6] [online] [cit. 2011-01-06] Dostupný z WWW <:https://www.servis24.cz/stat/ebanking/s24/help/cs/ib_trn_sms_aut.html>.

[7] [online] [cit. 2011-02-15] Dostupný z WWW: <http://download.alsoft.cz/vasco/pdf/Digipass_Go_3.pdf>.

[8] [online] [cit. 2011-02-15] Dostupný z WWW: <http://www.vasco.com/Images/DP%20270_april11.pdf>.

[9] [online] [cit. 2011-02-15] Dostupný z WWW: <http://www.vasco.com/Images/DP_for_Mobile_3.0.pdf>.

[10] PETERKA, J. Báječný svět elektronického podpisu. [online] 2011 no.13 [cit. 2011-03-25] Dostupný z WWW: <http://public.nic.cz/files/bajecny_svet/peterka_bs.pdf>.

[11] [online] [cit. 2011-02-18] Dostupný z WWW: <http://www.hoax.cz/phishing/>.

[12] [online] [cit 2011-02-18] Dostupný z WWW: <http://cs.wikipedia.org/wiki/Phishing>.

[13] [online] [cit 2011-02-16] Dostupný z WWW: <http://cs.wikipedia.org/wiki/Pharming>.

[14] [online] [cit 2011-03-03] Dostupný z WWW:
<http://cs.wikipedia.org/wiki/Man_in_the_middle>.

Seznam zkratek:

ANSI	-	American National Standards Institute
Apod.	-	a podobně
Atd.	-	a tak dále
B2B	-	Business-to-Business
B2C	-	Business-to-Customers
CRL	-	seznam zneplatněných certifikátů
EMV	-	Europay, MasterCard and VISA
E-podpis	-	Elektronický podpis
HTTPS	-	Hypertext Transfer Protocol Secure
HW	-	Hardware
IB	-	Internet Banking
IEEE	-	Institute of Electrical and Electronics Engineers
IETF	-	Internet Engineering Task Force
IP adresa	-	Internetový protokol
ISO	-	International Organization for Standardization
IT	-	Information technology
MAC	-	Message Authenication Code
MITB	-	Man In The Middle
MITM	-	Man In The Browser
NIST	-	National Institute of Standards and Technology
OTP	-	One-Time Password
PCI	-	Peripheral Component Interconnect
PCMCIA	-	Personal Computer Memory Cards International Association
PIN	-	Personal identification number
PKCS	-	Public Key Cryptographic Standards
PKI	-	Public Key Infrastructure
RFID	-	Radio-frequency identification
SCSII	-	Small Computer System Interface
SECG	-	Standards for Efficient Cryptography Group
SSL	-	Secure Sockets Layer
SW	-	Software

Prohlášení o využití výsledků bakalářské práce

Prohlašuji, že

- jsem byla seznámena s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou (bakalářskou) práci užít (§ 35 odst. 3);
- souhlasím s tím, že bakalářská práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že bibliografické údaje o bakalářské práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, bakalářskou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne ……

……

jméno a příjmení studenta

Adresa trvalého pobytu studenta:

…….